(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2000－78667
（P2000－78667A）
(43)公開日　平成12年３月14日(2000.3.14)

(51)Int.Cl.'		識別記号	FI		テーマコード'（参考）
Ｈ０４Ｑ	7/38		Ｈ０４Ｂ　7/26	１０９Ｒ	
	7/34			１０６Ａ	
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ　9/00	６０１Ｂ	

審査請求　未請求　請求項の数16　ＯＬ　（全 11 頁）

(21)出願番号　特願平11－204782

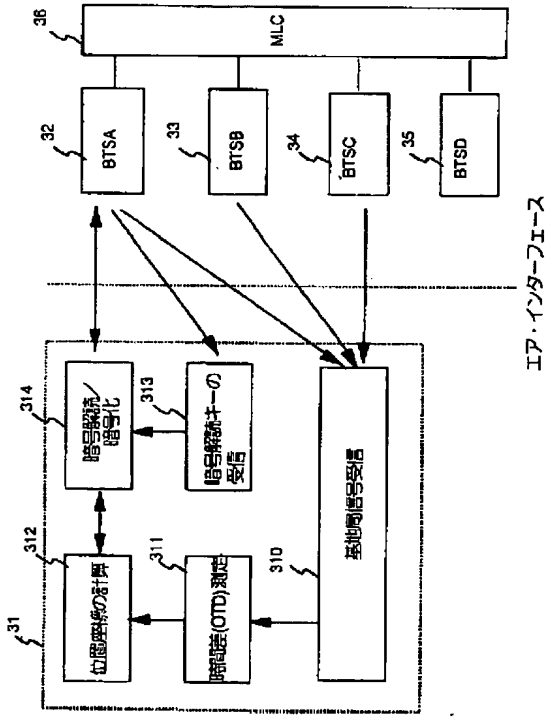
(22)出願日　平成11年７月19日(1999.7.19)

(31)優先権主張番号　９８１６３８
(32)優先日　平成10年７月17日(1998.7.17)
(33)優先権主張国　フィンランド（ＦＩ）

(71)出願人　591275137
ノキア　モービル　フォーンズ　リミテッド
NOKIA MOBILE PHONES LIMITED
フィンランド　02150　エスプー　ケイララーデンティエ　４
(72)発明者　ピリーレ　ハンヌ
フィンランド　エフイーエン－20660　リットイネン　カーリオリンネ　４
(74)代理人　100059959
弁理士　中村　稔　（外９名）

(54)【発明の名称】　移動通信システムにおいてサービスを管理する方法及び装置

(57)【要約】　（修正有）
【課題】移動通信システムの管理方法及び装置、移動局、及びインテリジェント・モジュールに関する。
【解決手段】本発明は、移動局から暗号化されたデータを複数の移動局に同時転送することにある。その暗号化は、移動局に個別に転送されるキーに基づく。移動局の位置は複数の基地局からの受信信号の時間差に基づいて測定される。該位置データは、該位置データの暗号解読に必要な暗号解読キーをオペレータが送った移動局だけが該位置データを利用できるように、暗号化された形で移動局に転送される。暗号解読キーは、各移動局に個別に転送される。暗号解読は移動局のインテリジェント・モジュールで行われるので機密性が保たれる。課金性だけが唯一の要件であるならば、暗号解読及び位置計算は移動局内の別の場所で行われても良い。



【特許請求の範囲】
【請求項１】　同じ情報が唯一の送信チャネルで複数の移動局に転送される移動通信システムでサービスを管理する方法であって、複数の移動局に同時に転送される前記情報は暗号化され、その暗号化は、各移動局に別々に転送される暗号解読キーを使って実行されることを特徴とする方法。
【請求項２】　前記暗号化は、該移動通信システムから移動局に転送される暗号解読キーを利用することを特徴とする請求項１に記載の方法。
【請求項３】　前記暗号解読キーは移動局に個別に転送されることを特徴とする上記請求項のいずれかに記載の方法。
【請求項４】　前記暗号解読キーは可変であることを特徴とする請求項２又は３に記載の方法。
【請求項５】　前記の同時に転送される情報及び暗号解読キーの暗号解読はインテリジェント・モジュールで実行されることを特徴とする上記請求項のいずれかに記載の方法。
【請求項６】　移動局（３１）の位置を測定する方法であって、この方法では：
－　少なくとも２つの基地局（３２、３３、３４、３５）から受信された信号間の観測時間差（ＯＴＤ）が該移動局で測定され；
－　前記の少なくとも２つの基地局の位置情報が該移動局（３１）に転送され；
－　該移動局（３１）の位置座標は前記の少なくとも２つの基地局の前記時間差（ＯＴＤ）及び位置情報に基づいて該移動局（３１）において計算され；
－　前記基地局の位置情報は暗号化された形で移動局に転送されることを特徴とする方法。
【請求項７】　該移動局の位置についての計算は該移動局のインテリジェント・モジュールで実行されることを特徴とする請求項６に記載の方法。
【請求項８】　同じ情報が唯一の送信チャネルで複数の移動局に転送される移動通信システムであって、前記移動通信システムは、複数の移動局に同時に転送される前記情報を、暗号解読キーを使って、暗号化するための手段と、その暗号化に使われる該暗号解読キーを各移動局に別々に転送するための手段とを有することを特徴とする移動通信システム。
【請求項９】　複数の基地局（３２、３３、３４、３５）及び移動局（３１）を含む移動通信システムを含む、移動局位置測定方法であって：
－　少なくとも２つの基地局（３２、３３、３４、３５）から受信された信号間の観測時間差（ＯＴＤ）が該移動局で測定され；
－　前記の少なくとも２つの基地局の位置情報が該移動局（３１）に転送され；
－　該移動局（３１）の位置座標は前記の少なくとも２つの基地局の前記時間差（ＯＴＤ）及び位置情報に基づいて該移動局（３１）において計算され；
－　前記基地局の位置情報を暗号化された形で移動局に転送するようになっていることを特徴とする移動局位置測定方法。
【請求項１０】　サービスに関連する情報を放送チャネルで受け取るための手段を有する移動局であって、暗号解読キーを使って前記情報を暗号解読するための手段と、前記移動局に割り当てられたチャネルで前記暗号解読キーを受け取るための手段も有することを特徴とする移動局。
【請求項１１】　当該移動局の位置を測定する目的のために：
－　少なくとも２つ基地局（３２、３３、３４、３５）から信号を受信するための手段（３１０）と；
－　受信された信号間の観測時間差（ＯＴＤ）を測定するための手段と；
－　前記の少なくとも２つの基地局の位置情報を該移動局（３１）に転送するための手段と；
－　前記の少なくとも２つの基地局の前記時間差（ＯＴＤ）及び位置情報に基づいて該移動局（３１）の位置を測定するための手段（３１２）とを有する移動局であって、この移動局は：前記基地局位置情報を暗号解読するための手段（３１４）も有することを特徴とする移動局。
【請求項１２】　位置情報を暗号解読するために暗号解読キーを基地局から受け取るための手段を有することを特徴とする請求項１１に記載の移動局。
【請求項１３】　前記移動局位置情報をシステムに送るための手段を有することを特徴とする請求項１１又は１２に記載の移動局。
【請求項１４】　移動局のインテリジェント・モジュールであって、このインテリジェント・モジュールは、該移動局からサービスに関連する暗号化されている情報を受け取るための手段を含んでおり、更に、暗号解読キーによって前記情報を暗号解読するための手段と、前記暗号解読キーを該移動局から受け取るための手段とも含んでいることを特徴とするインテリジェント・モジュール。
【請求項１５】　暗号解読キーを受け取り、前記暗号解読キーを使って基地局位置情報を暗号解読するための手段を含んでいることを特徴とする、移動局のインテリジェント・モジュール。
【請求項１６】　時間差情報と基地局位置情報とに基づいて該移動局の位置を計算するための手段を含んでいることを特徴とする請求項１５に記載のインテリジェント・モジュール。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、移動通信システム

においてサービスを管理する方法及び装置、移動局及び移動局のインテリジェント・モジュールに関する。本発明は、移動局のための位置測定方法に有利に適用される。この方法は、アナログ及びディジタルの移動通信システムに応用可能である。その様なシステムの例はディジタル時分割に基づくＧＳＭ（Global System for Mobile Communications（移動通信用広域システム））である。

【０００２】

【従来の技術】移動局の位置情報を多くの目的に使うことができる：

－　移動局の位置に応じて通話の値付けを行うことができ、その場合、例えばホームエリアからなされた通話を比較的に安くすることができる；

－　移動局から非常電話がかけられたとき、その電話をかけた移動局の位置を測定することが可能である（この機能は、或る国では関係当局が必要とするものである）；

－　移動局のユーザーは、例えば旅行しているときなどには、自分がいる場所に関する情報を必要とすることがある；

－　関係当局は、位置情報を使って、例えば盗まれた移動局の位置を突き止めたり、行方不明になった人を捜し出すことができる。

【０００３】位置測定プロセスはシステムでのデータのやりとりを必要とするので、オペレータは使用に応じて位置測定サービスに料金を課すことができなければならない。更に、例えばユーザーがホームエリア以外の場所にいるときにホームエリア割引をしてもらおうとして位置情報を偽造するようなことが不可能となるように、位置測定プロセスは安全なものでなければならない。更に、システムに関連する情報を第三者に伝えることは必ずしもオペレータのためにはならないので、データは機密であっても良い。

【０００４】衛星から受信される信号の利用に基づく全地球測位システム（ＧＰＳ）は位置測定を目的として広く使われている。この仕組みは、ＧＰＳ受信装置を移動局に付加することを必要とし、その結果として追加の相当のコストが必要となる。従って、全ての移動電話のための位置測定システムでは、一部の移動局モデルはＧＰＳ受信装置も含んでいるけれども、移動局と基地局との間で転送されるセルラーシステム自体の信号を利用して移動局の位置を測定するのが好ましい。

【０００５】基地局から移動局までの距離を該移動局と基地局との間で伝送される信号の伝播遅延に基づいて測定する方法が刊行物[1] WO 92/05672から知られている。図１は、その方法の作動原理を示している。基地局１で移動局１４から送られた信号の伝播遅延を測定することにより、移動局と基地局との間の推定距離ｄ１が得られる。距離測定の精度の故に、移動局の推定位置は測定の幅が遅延時間測定精度に依存するリング状の領域の中にある。該移動局と他の基地局との間での信号について、同じ伝播遅延測定を行うことができる。測定の結果として、測定に関わる各基地局につき１つずつのリング状位置領域が得られる。図１に示されている状況では、移動局及び基地局１１の間、移動局と基地局１２との間、並びに移動局と基地局１３の間での伝播遅延は、リング状領域１６、１７及び１８に対応する推定距離ｄ１、ｄ２、及びｄ３を与える。これらのリングは領域１９で交差し、これが３つの伝播遅延測定から得られた移動局の位置領域である。この様に、移動局の位置を、寸法等級が測定精度に等しい領域であると判定することができる。上記の方法では、位置測定は実質的にシステムによって実行され、測定を実行するために移動局に特別の機能は不要である。

【０００６】移動局と基地局との間の信号から測定された伝播遅延に基づく方法の欠点は、移動局の位置についての情報の精度が上記アプリケーションの全てについて充分であるような精度で伝播遅延を簡単に測定することはできないということである。更に、移動局は、伝播遅延が測定されるべき全ての基地局とアップリンク接続を確立しなければならない。位置情報を絶えず更新し続けなければならないとすると、位置情報に関連するデータのやりとりは移動通信システムの接続容量に相当の負担を課すことになる。更に、データ通信の量が多いので、測定が遅くなる。移動局の絶対タイミング精度におけるエラーが、得られる位置測定結果にエラーをもたらすことも、この方法の問題である。

【０００７】図２は、移動局或いはシステムが測定を実行することのできる時間差に基づく測定の動作原理を示している。移動局に複数の基地局から（図２の場合には３つの基地局ＢＴＳ１、ＢＴＳ２、及びＢＴＳ３から）信号を受信させるとする。移動局の位置についての推定結果は、複数の基地局から受信される信号間に観測される時間差（Observed Time Difference (OTD)）によって決定され、この場合、２つの基地局から受信された信号間の時間差によって、移動局と第１基地局との間の距離ｄ１と、移動局と第２基地局との間の距離ｄ２との差ｄ１－ｄ２を計算することが可能である。距離差の値がｄ１－ｄ２に等しい、移動局が存在する可能性のある場所は、双曲線状の曲線を構成し、その曲線は、移動局が存在する可能性のある場所を表す。図２において、この曲線は破線で描かれている。測定結果には一定のエラー・マージンがあるので、移動局の位置領域は実際は２つの双曲線の間の帯であり、その帯の幅は測定結果のエラー・マージンに依存する。少なくとも３つの基地局ＢＴＳ１、ＢＴＳ２及びＢＴＳ３から信号が受信されるとき、結果は、複数の位置領域Ａ１２、Ａ１３、及びＡ２３であり、移動局はこれらの領域の交差箇所に位置する。時間差測定に加えて例えば伝播遅延測定などの他の方法を

使用しないならば、限られた位置領域を決定するためには少なくとも３つの基地局から受信される信号について時間差測定を行う必要がある。他の追加の方法を使用するのであれば、２つの基地局だけから受信された信号について時間差測定を利用することが可能である。従って、図２に描かれている測定原理を使用するとき、移動局の位置を移動局又はシステムによって計算することができる。

【０００８】特許文献[2] FI 101445から、移動局が基地局から受信した信号の時間差を測定して、測定された時間差のデータを移動通信システムに送信する解決策が知られている。移動通信システムの移動位置測定センターは、測定された時間差のデータ、基地局位置座標及び基地局実時間差（Real Time Data (RTD)）に基づいて移動局の位置を計算する。この解決策には、時間差データを移動局からシステムへ送らなければならず、そのためにアップリンク方向のデータ転送容量に負担がかかるという欠点がある。

【０００９】文献[1]及び[2]に開示されている解決策では、移動局の位置はセルラーシステムによって計算される。その後、その位置情報を必要とするアプリケーションが移動局にあるならば、移動局位置情報はシステムから移動局へ特別のメッセージで送られなければならない。ユーザーが位置情報を頻繁に必要とするならば、大量のデータ転送がダウンリンク方向にも行われることになる。他の欠点は、位置情報は始めにシステムによって計算されなければならないので、ユーザーは実時間位置情報を受け取ることができないということである。

【００１０】文献[3] EP 398773から知られている解決策では、移動局は移動通信システムから該移動局の周囲の地域にある複数の基地局のタイミング差と位置座標とに関する情報を受け取る。その後、移動局は前記の複数の基地局から受け取った信号のタイミング差を測定し、その測定されたタイミング差、基地局タイミング差及び位置座標に基づいて、該移動局に蓄積されている位置測定アルゴリズムを使って該移動局の位置を判定する。前記文献は、この方法においてシグナリングを具体的にどの様に実行するのかを詳しく説明していない。この解決策の欠点は、複数の基地局から送られる信号に基づいて移動局が独自に位置測定を実行できるのでオペレータは位置測定サービスについての料金をユーザーに請求できないということである。この解決策の別の欠点は、システムに送られる位置情報をユーザーが偽造できるので、この位置測定方法は多くのアプリケーションのためには充分に信頼できる方法ではないということである。

【００１１】移動局の位置情報を多くのアプリケーションで利用できるけれども、従来技術の解決策はアプリケーションの全ての要件を満たすものではない。

【００１２】

【発明が解決しようとする課題】本発明の目的は、従来技術に関連する上記の欠点を無くして、移動通信システムにおいてサービスを管理するための解決策を提供することである。この解決策により、位置測定サービスの課金性、信頼性、及び機密性に関する要件を満たす、移動局の位置情報を測定する方法及び移動局を実現することができる。

【００１３】

【課題を解決するための手段】本発明の着想は、移動局でサービスのために必要なデータを暗号化された形で数台の移動局に同時に転送するということである。暗号化は、移動局に個別に送られる暗号解読キーの使用に基づく。

【００１４】移動局の位置測定に応用する場合、このことは、移動局の位置が、該移動局において、少なくとも２つ（好ましくは少なくとも３つ）の基地局から受信された信号間のタイミング差に基づいて、前記基地局の位置情報を用いて測定されるということを意味する。位置情報は、基地局位置座標、実時間差（ＲＴＤ）データ及び、移動局の位置を測定するのに必要な他の基地局に関連するデータを意味する。基地局位置情報は、該位置情報の暗号解読に必要な暗号解読キーをオペレータが送った移動局だけが該位置情報を使えるように、暗号化された形で移動局に転送される。暗号解読キーは好ましくは個別に、暗号化された形で移動局に転送される。暗号解読キーは変更されても良く、その場合には新しい暗号解読キーは有利には位置更新と関連して移動局に転送されるが、それはＧＳＭで使われる手順である。

【００１５】暗号解読キー及び位置情報の転送時に、インテリジェント・モジュール（例えば、スマートカード）に蓄積されているアルゴリズムを使って位置情報も計算できるように、暗号解読はインテリジェント・モジュールで行われるのが有利である。暗号解読キーが暗号化されて、その暗号解読キーの暗号解読がインテリジェント・モジュールで行われるのであれば、結果としてサービス課金性及びデータ機密性の両方が得られる。必要なのは課金性だけであるならば、暗号解読及び位置情報計算は移動局においてインテリジェント・モジュール以外の場所で行われても良い。更に、移動局位置情報を必要とするアプリケーションがシステムにあるのならば、システムに送られる位置情報は、送信される前にインテリジェント・モジュールで暗号化されても良い。

【００１６】移動局の位置が該移動局で計算されるので、本発明は、音声モード、データ・モード及び待機モードでの実時間連続位置計算を容易にする。位置情報は暗号化されるので、はっきりと位置測定サービスを注文したものだけが位置測定サービスを利用できるようにすることが可能であり、このサービスの利用を有料にすることができる。課金は、暗号解読キーの引き渡しに基づいて行われても良く、或いは例えば月毎の請求の形をとっても良い。本発明の解決策の利点は、もし当該データ

が暗号化されていない形となっている唯一の場所が移動局のスマートカードであるならば、ユーザーは、例えば、位置測定プロセスに使われるデータも、システムに送られる位置情報も偽造することができないことである。

【００１７】情報が複数の移動局に移動通信システムの唯一の送信チャネルで同時に転送されるようになっている、サービスを管理するための方法は、複数の移動局に同時に転送される前記情報が暗号化され、各移動局に別々に転送される暗号解読キーを使ってその暗号化が実行されることを特徴とする。

【００１８】移動局の位置を測定する本発明の方法においては、

－　少なくとも２つの基地局から受信された信号間の観測時間差が移動局で測定され、

－　前記の少なくとも２つの基地局の位置座標が該移動局に転送され、

－　該移動局の位置座標が該移動局において前記の少なくとも２つの基地局の前記時間差及び位置座標に基づいて計算されるようになっており、

－　この方法は、前記基地局位置座標が暗号化された形で移動局に転送されることを特徴とする。

【００１９】複数の基地局及び移動局を含む移動通信システムを有する、本発明の移動局位置測定システムにおいては、

－　少なくとも２つの基地局から受信された信号間の観測時間差が移動局で測定され、

－　前記の少なくとも２つの基地局の位置座標が該移動局に転送され、

－　該移動局の位置座標が該移動局において前記の少なくとも２つの基地局の前記時間差及び位置座標に基づいて計算されるようになっており、

－　このシステムは、前記基地局位置座標が暗号化された形で移動局に転送されるようになっていることを特徴とする。

【００２０】サービスに関連する情報を放送制御チャネルで受信するための手段を有する本発明の移動局は、前記情報を暗号解読キーによって暗号解読するための手段と、前記移動局に割り当てられたチャネルで前記暗号解読キーを受け取るための手段とを有することを特徴とする。

【００２１】本発明の移動局は、当該移動局の位置を測定する目的のために、

－　少なくとも２つの基地局から信号を受信するための手段と、

－　受信された信号間の観測時間差を測定するための手段と、

－　前記の少なくとも２つの基地局の位置座標を該移動局に転送するための手段と、

－　該移動局の位置座標を前記の少なくとも２つの基地局の前記時間差及び位置座標に基づいて測定するための手段とを有し、この移動局は、前記基地局位置座標情報を暗号解読するための手段も有することを特徴とする。

【００２２】移動局からサービスに関連する暗号化されている情報を受け取るための手段を有する本発明の移動インテリジェント・モジュールは、暗号解読キーを使って前記情報を暗号解読するための手段と、前記暗号解読キーを移動局から受け取るための手段とも有することを特徴とする。

【００２３】本発明の移動スマートカードは、基地局から受信された情報に基づいて基地局位置座標データの暗号化に使われる暗号解読キーを作るための手段を有することを特徴とする。

【００２４】本発明の好ましい実施態様が従属請求項で開示されている。

【００２５】次に、添付図面を参照して本発明をいっそう詳しく説明する。

【００２６】

【発明の実施の形態】図１及び２については従来技術の解説との関係で既に説明した。次に図３を参照して本発明の位置測定方法の動作原理を開示し、次に図４～８を参照して、本発明の方法に関連するシグナリング・ステップを実行する方法をいっそう詳しく説明する。本発明の移動局及びインテリジェント・モジュールの不可欠のコンポーネントが図９及び１０に示されている。最後に、従来技術と比べて本発明の解決策がどんな利点を持っているか説明する。図解されている実施態様の説明において、M. Mouly、M-B. Pautetの“移動通信のためのＧＳＭシステム、１９９２(The GSM System for Mobile Communications, 1992)”に詳しく開示されているＧＳＭシステムを参照する。

【００２７】２つの基地局から移動局により受信された信号間の時間差を観測時間差（Observed Time Difference (OTD)）と称する。ＯＴＤの測定値は、ハンドオーバー時に新たにサービスをするようになる基地局のクロック信号に移動局を同期させるのに利用され、ＯＴＤ測定方法は従来技術から知られている。移動局は２つの基地局から同時に信号を受信することはできないので、ＯＴＤは２段階で測定される。始めに、移動局は、自分自身のタイミングと、第１の基地局から受信した信号のタイミングとの第１時間差を測定する。次に移動局は自分と第２基地局との第２時間差を測定する。ＯＴＤはこの第１及び第２の時間差の差に等しい。ＯＴＤの測定は、次の文献：[5] prETS 300579: GSM 05.10バージョン4.4.1, 欧州ディジタルセルラー通信システム（フェーズ２）；無線サブシステム同期化、欧州通信規格協会、１９９４、１４ｐｐ（prETS 300579: GSM 05.10 version 4.4.1,European digital cellular telecommunications system (Phase 2; Radio subsystem synchronisation, European Telecommunications Standars Institute,19

94，14pp）に詳しく記載されている。

【００２８】図３は、本発明の位置測定システムの動作原理を図解している。それは移動通信システムを含んでおり、そのうちの４つの基地局ＢＴＳＡ（３２）、ＢＴＳＢ（３３）、ＢＴＳＣ（３４）及びＢＴＳＤ（３５）が描かれている。図解されているものの場合、基地局ＢＴＳＡは、移動局３１にサービスをする基地局である。サービスをする基地局ＢＴＳＡは位置測定プロセスで使われる暗号解読キー３１４に関する情報を移動局３１に送り、これで移動局は基地局から受け取った位置情報を暗号解読する。この位置情報は、基地局から移動局に例えばＳＭＳセル放送メッセージ(a SMS Cell Broadcast message）で送られる。

【００２９】移動局３１は基地局ＢＴＳＡ、ＢＴＳＢ及びＢＴＳＣからタイミング信号を受信ブロック３１０で受け取る。移動局は異なる基地局から受け取った信号間の時間差をブロック３１１で測定し、それをブロック３１２に送り、このブロックは移動局の位置座標を計算する。必要ならばその位置座標は更にサービスをする基地局に転送され、そのとき基地局情報の転送の場合と同じ種類の暗号化を使用することが可能である。基地局への転送は、例えば、システムによって移動局へ送られる要求に対する応答として実行される。

【００３０】サービスをする基地局から移動局の位置座標を移動通信システムの移動位置測定センターＭＬＣ（３６）に更に転送することができ、ここでいろいろなアプリケーションが該位置情報にアクセスし得るようになる。移動位置測定センターは移動通信システムの他の部分と関連して置かれていても良く、これは独立のユニットでなくても良い。時間差に基づく位置測定に加えて、システムは他の方法を使用することもできる。

【００３１】基地局位置情報を機密に保ちたいならば、暗号解読及び位置計算は移動局のインテリジェント・モジュールで行われても良い。その場合には、図３の論理ブロック３１２－３１４はインテリジェント・モジュールの中にある。機密性が不要ならば、問題の機能は移動局３１内の別の場所で実行されても良い。

【００３２】移動局は、要求に対する応答として、或いは位置更新と関連して、基地局から暗号解読キーを受け取ることができる。図４は、定期的位置更新と関連して暗号解読キーを移動局に転送する本発明の方法を図解している。移動局は移動交換センターに[定期的位置更新要求]を送り、システムは[位置更新肯定応答]を送り返す。移動局のユーザー／加入者が位置測定サービスを利用する権利を持っているならば、暗号解読キー又はそれを作るのに必要な情報は前記肯定応答メッセージと関連して転送される。更に、その暗号解読キーについての有効期間が与えられても良い。

【００３３】図５は、位置更新が異なる時間に行われる数台の移動局ＭＳ１、ＭＳ２及びＭＳ３への暗号解読キーの転送を図解している。もし暗号解読キーの転送が定期的位置更新と関連して行われるのであれば、暗号解読キーの変更を位置更新期間より長い期間毎に実行するのが好都合である。その場合、新しい暗号解読キーを暗号解読キーの変更より前に全ての移動局に転送することができる。移動局が閉じられていてオンに切り換えられるのであれば、次の位置更新より前に暗号解読キーの次の変更が行われるならば、第１の位置更新で現在の暗号解読キーと次の暗号解読キーとの両方を転送することが可能である（図５の移動局ＭＳ３を参照）。一方、始動時に特別の手続きが不要となるように、常に現在の暗号解読キーと次の暗号解読キーとを転送することができる。

【００３４】図６は、放送メッセージでの位置情報の移動局への転送のシグナリング流れ図である。ステップ６１で、移動位置測定センターＭＬＣは、必要な位置情報を暗号化し、その情報をショートメッセージ・サービス・セル放送センターＣＢＣに送る。ステップ６２で、ショートメッセージ・サービス・セル放送センターＣＢＣは位置情報を基地局コントローラＢＳＣに送り、このＢＳＣはそれを更に基地局ＢＴＳに送る（ステップ６３）。ステップ６で基地局ＢＴＳは位置情報を更にショートメッセージ・サービスＳＭＳ放送チャネルで移動局ＭＳに送る。

【００３５】図７は、本発明の解決策と関連して使用することのできる位置情報メッセージを示している。キー番号７１は、現在の暗号解読キーを決定するために使われる。移動局は、キー番号が変化した時点から新しい暗号解読キーを使い始める。メッセージ番号７２は、暗号化アルゴリズムで入力パラメータとして使われる。公用データ７３は、ＯＴＤ値だけを測定して、それを位置計算のためにシステムに送る移動局が必要とする公用情報を含むことがある。その様な情報は、例えば、ＯＴＤ測定に適する基地局のリスト、チャネル番号、基地局識別情報、基地局により使用されるバースト長さ或いは可能なＲＴＤ値を含む。暗号化されたデータ７４は、位置測定サービスを利用する権利を有する移動局だけが利用できる情報を含んでいる。それらのデータは、基地局の座標と、正確なタイミング或いはＲＴＤの値など、位置計算に必要な基地局位置情報を含んでいる。更に、メッセージは、特に、該メッセージで暗号化が行われているかどうかを示すヘッダ（図示されていない）を含んでいる。

【００３６】図８は、移動局が新しいビジター位置レジスターＶＬＲの領域に入るときに位置更新と関連して暗号解読キーが移動局に転送される場合のシグナリング流れ図である。ステップ８１で、移動局ＭＳは位置更新手続きを開始する。ステップ８２で、新しい移動交換センターＭＳＣ／ビジター位置レジスターＶＬＲは、前のビジター位置レジスターに関する情報を移動局から要求し、ホーム位置レジスターＨＬＲにビジター位置レジス

ターが変更されたことを知らせる（ステップ８３）。ステップ８４で、ホーム位置レジスターは、前のレジスターについての“位置をキャンセルする”手続きを実行して、加入者データを新しい移動交換センター／ビジター位置レジスターに送り（ステップ８５）、新しい移動交換センター／ビジター位置レジスターはそれを肯定応答する（ステップ８６）。ステップ８７で、新しい移動交換センター／ビジター位置レジスターは移動局の位置更新要求を肯定応答する。もし移動局のユーザーが、移動局に基づく位置測定サービスを利用する権利を持っているならば、その肯定応答は、放送される位置情報についての現在の暗号解読キーと、場合によっては次の期間についての暗号解読キーとを含んでいる。

【００３７】図９は、セルラーシステムにおける本発明の移動局９００の略ブロック図である。次に、始めにこの移動局の普通の機能を説明する。移動局は、基地局によって送信された無線周波数（ＲＦ）信号を受信するアンテナ９０１を有する。受信されたＲＦ信号は、例えばデュプレックス・フィルター９０２を通してＲＦ受信装置９１１に送られ、ここで信号は増幅されディジタルに変換される。この信号は、次にブロック９１２で検出されて復調され、ブロック９１３でデコーディングされる。その後、信号は、送信された情報が音声であるかそれともデータであるかに応じて処理される。データはそのまま移動局のメモリー９０４に蓄積され得る。本発明に従って、基地局から受信された位置データ又はその他のサービス・データと暗号解読キーとは制御ユニット９０３又はインテリジェント・モジュール９４０で処理される。処理された音声信号はイヤホンに送られる。制御ユニットは、制御ユニット／メモリーに蓄積されているプログラムに従って上記の受信ブロックを制御する。

【００３８】移動局からの送信は、例えば次のように行われる。始めに、ブロック９２１で、制御ユニット９０３は、システムに従って、マイクロホンから到来するオーディオ信号をエンコーディングする。送信される情報は、本発明の移動局位置情報などのデータであっても良い。エンコーディングされたデータはブロック９２２でバーストに編成され、それはブロック９２３でＲＦ信号に変調されて増幅される。この送信されるＲＦ信号は例えばデュプレックス・フィルター９０２を通してアンテナ９０１に送られる。これらの処理及び送信の機能も制御ユニット９０３によって制御される。更に、図９は、普通の移動局に付いているキーパッド９３１及びディスプレイ９３２も示している。

【００３９】本発明に従ってそれらの機能を設けるために、プログラムが制御ユニット／インテリジェント・モジュールに蓄積されており、それに基づいて制御ユニットは本発明に従って移動局の他のブロックを制御する。

【００４０】図１０は、インテリジェント・モジュール１４０ＳＩＭのブロック図である。制御ユニット１３０ＣＰＵは、プログラム・メモリー１４２ＲＯＭに蓄積されているプログラム・コードに従ってインテリジェント・モジュールＳＩＭの動作を制御する。データ・メモリー１４４ＥＥＰＲＯＭに種々のユーザー固有データを蓄積しておくことが可能であり、そのデータは、動作電圧がＳＩＭモジュール１４０から除去されても該メモリーに残存する。データを一時的に蓄積しておくために作業メモリー１４６ＲＡＭを使うことができる。バス・アダプター１２０ＤＡＴＡ－Ｉ／Ｏは、インテリジェント・モジュールＳＩＭの移動局インターフェース（制御及びデータＩ／Ｏ）をインテリジェント・モジュールＳＩＭの内部バス３６０に適合させる。更に、ＳＩＭモジュールは送信されるデータ及び蓄積されるデータを暗号化したり暗号解読したりするための暗号化ブロック１５０を有する。本発明の機能を中央処理装置１３０に実行させることができるように、本発明に関連するアルゴリズム及びプログラムを蓄積しておくために上記のメモリー・ユニットを使うことができる。更に、インテリジェント・モジュールＳＩＭのいろいろなブロックの目的は、従来技術に従って、加入者の識別に必要なデータを管理すること、並びに、ショートメッセージ、音声ダイヤル・コード及びその他のユーザー固有の情報を蓄積しておくための記憶手段として作用することである。

【００４１】図９は、本発明のシステムで利用されるセルラーシステム・コンポーネントを更に示している。ＲＦ信号の送信及び受信は基地局９５１のアンテナ９５０を通して実現される。基地局９５１から基地局コントローラ９５２を介して交換局９５３への接続が確立される。交換局９５３は、システムの他の基地局システムとは別に、特に、ホーム位置レジスター９５４及び公衆交換電話回線網ＰＳＴＮにも接続されている。ホーム位置レジスターは、特に、本発明のサービスへのアクセス権に関する情報を蓄積する。

【００４２】移動局の位置を測定する本発明の解決策は、従来技術と比べて次のような多くの利点を提供する：

－　位置測定プロセスに使われるデータは暗号化されて転送されるので、位置測定サービスのユーザーに利用料金を請求できる。

－　この解決策はエア・インターフェースに大きな追加負荷を課す結果をもたらさない。

－　この方法は、移動局のプロセッサに大きな追加の負荷を課す結果をもたらさない。

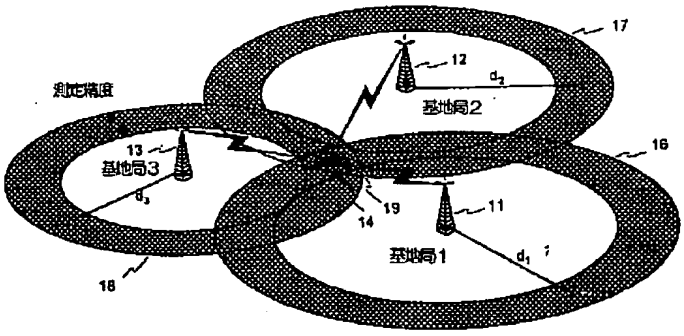
－　前述した理由により、位置測定を迅速に且つ短い間隔で実行することができる。

－　この方法は既存のネットワークに容易に導入され得るので、小さな修正が必要であるに過ぎない。

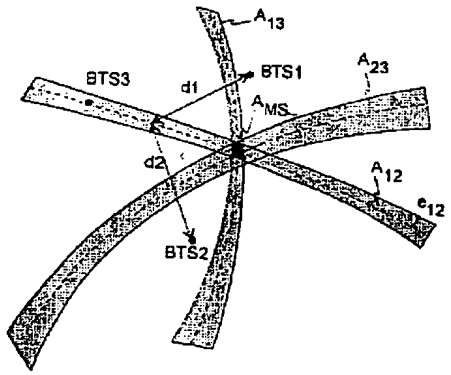
－　ＳＩＭカードを変更することによって位置測定アルゴリズムを簡単に更新できる；移動局の修正は不要である。

－　この方法を使って、静止している移動局及び移動中の移動局の両方の位置を測定することができる。
－　待機モード及び通話モードの両方において位置測定が実時間で作用する。
【００４３】本発明をディファレンシャルＧＰＳ位置測定システムと関連させて使用することも可能であることに留意するべきである。位置測定アルゴリズムが必要とするディファレンシャル・データは上記のようにして移動通信システムの基地局から暗号化されて入手され、移動局により計算される位置情報も暗号化された形でシステムに転送されることができる。
【００４４】以上、本発明の方法のアプリケーションを解説した。例えばアプリケーションの具体的詳細及び領域に関して、本発明の原理は、請求項により定義される発明の範囲内で当然に修正されて良い。
【００４５】特に、情報がダウンリンク方向にユーザーに放送される如何なるサービスを管理するためにも本発明の解決策を使えることに留意するべきである。問題のサービスで放送される情報は、暗号化された形で例えば放送チャネルで転送され、暗号解読キーは各移動局に別々に転送される。その様なサービスの１例はニュースを移動局に転送するサービスであり、その場合、ニュース情報を唯一のチャネルで全てのユーザーに送ることができ、暗号解読キーは、そのユーザーがそのサービスに申し込みをした移動局だけに転送される。これにより、送信容量に大きな追加負担を課すことなくユーザー従量課金が容易となる。
【００４６】以上の記述ではＧＳＭシステムにおける本発明の使用を説明したけれども、例えばＤＣＳ１８００／１９００（１８００／１９００ＭＨｚのディジタル通信システム）、米国で使われているＵＳ－ＴＤＭＡシステム、或いは日本で使われているディジタルＪＤＣシステムなど、他の、アナログ及びディジタルの両方の、通信システムに本発明を使用することが可能である。同様に、本発明は、ＷＣＤＭＡ（広帯域符号分割多元接続（Wide-band Code Division Multiple Access））などの将来型システムにも使用し得るものである。
【００４７】更に、本発明の方法は、前述した送信チャネル、シグナリング又はメッセージには限定されない。
【図面の簡単な説明】
【図１】基地局と移動局との間での伝播遅延を測定することに基づく従来技術の移動局位置測定方法を図解している。
【図２】時間差に基づく公知の位置測定方法を図解している。
【図３】本発明の位置測定システムを図解している。
【図４】暗号解読キーを移動局に転送するための本発明の方法を図解している。
【図５】複数の移動局への暗号解読キーの転送を図解している。
【図６】移動局への放送メッセージでの位置情報の転送のシグナリング流れ図である。
【図７】本発明の解決策に使うことのできる位置情報メッセージを示す。
【図８】移動局が新しいビジター位置レジスターＶＬＲの領域に入るときに位置更新と関連して移動局に暗号解読キーが転送される場合のシグナリング流れ図である。
【図９】本発明の移動局を示す。
【図１０】本発明のインテリジェント・モジュールを示す。
【符号の説明】
３１　移動局
３２、３３、３４、３５　基地局
３１２　位置座標計算ブロック
３１４　暗号解読キー受信ブロック

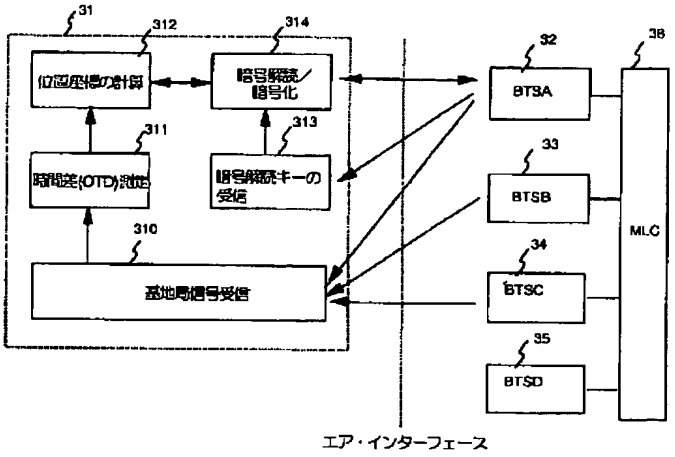
【図１】



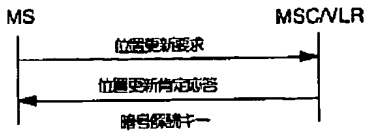
【図２】



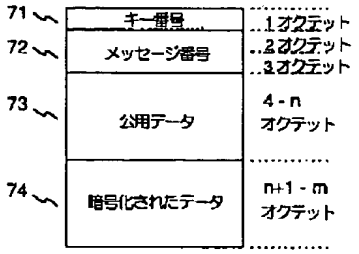
【図３】



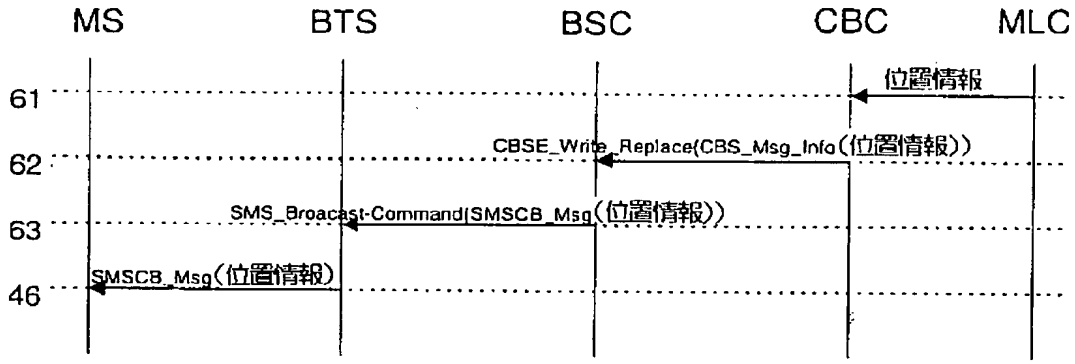
【図４】



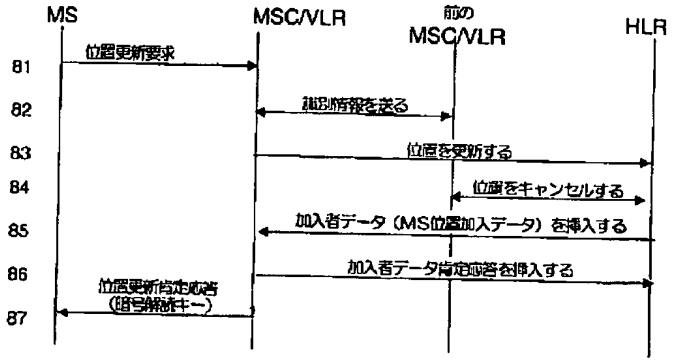
【図７】



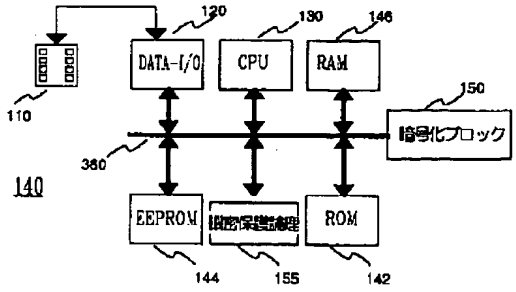
【図６】



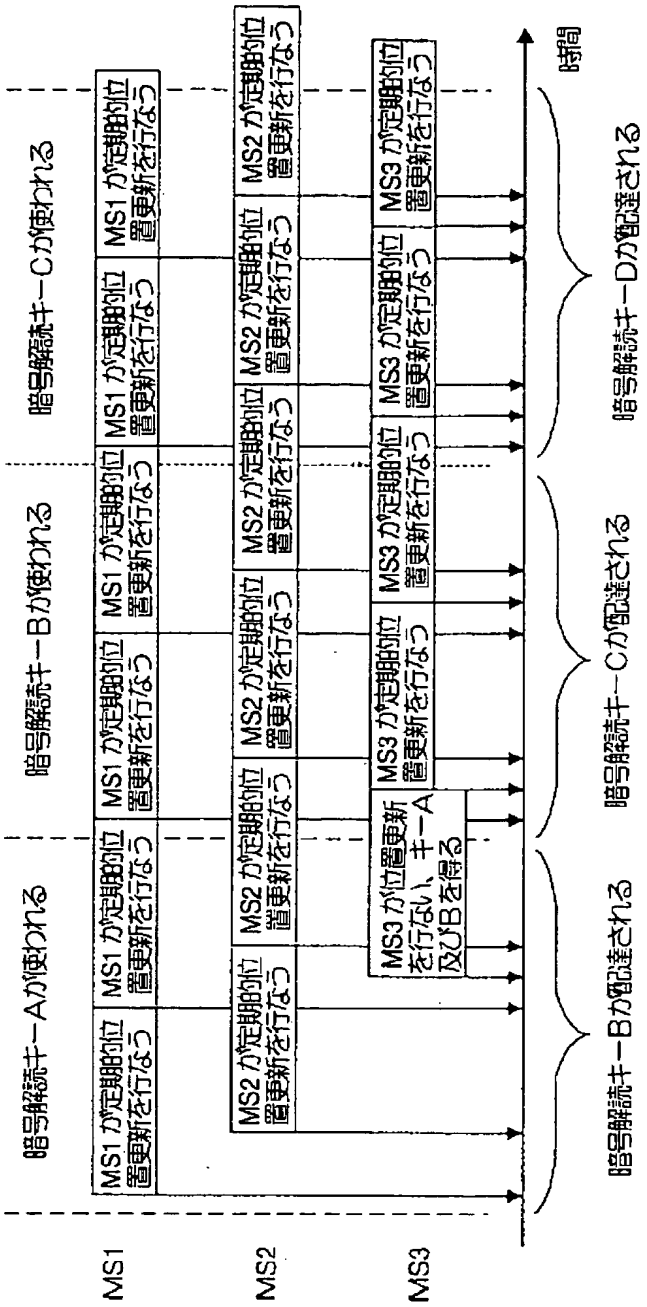
【図８】



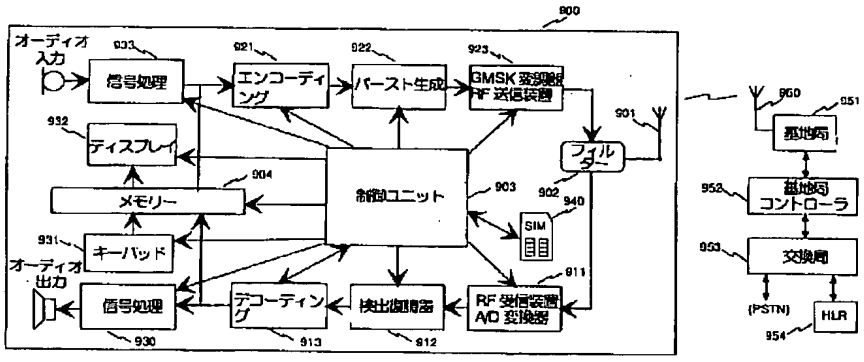
【図１０】



【図５】


暗号解読キーAが使われる
暗号解読キーBが使われる
暗号解読キーCが使われる
MS1
MS2
MS3
MS1が定期的位置更新を行なう
MS2が定期的位置更新を行なう
MS3が定期的位置更新を行なう
MS3が位置更新を行ない、キーA及びBを得る
暗号解読キーBが配達される
暗号解読キーCが配達される
暗号解読キーDが配達される
時間

【図９】


900
オーディオ入力
933
信号処理
921
エンコーディング
922
バースト生成
923
GMSK 変調器 RF 送信装置
901
フィルター
960
951
基地局
952
基地局コントローラ
953
交換局
(PSTN)
HLR
954
932
ディスプレイ
904
メモリー
制御ユニット
903
902
940
SIM
931
キーパッド
オーディオ出力
930
信号処理
913
デコーディング
912
検出復調器
911
RF 受信装置 A/D 変換器